Fig. 1

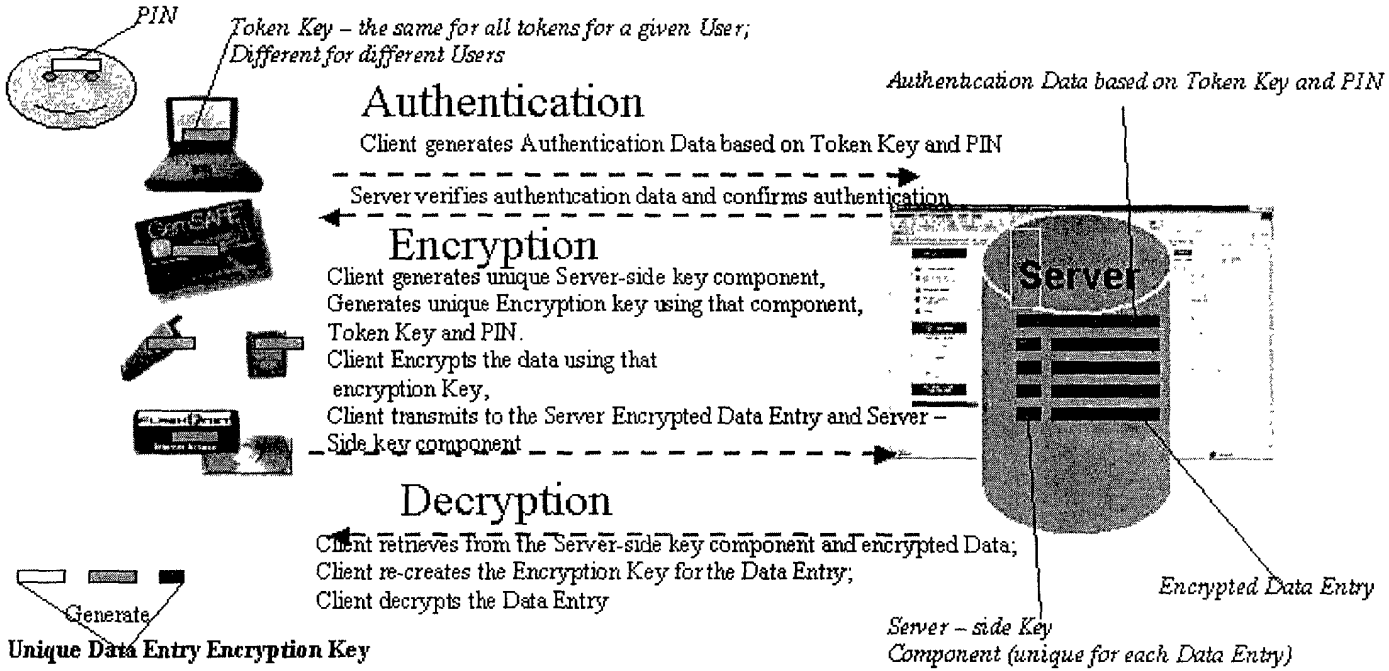

PIN
Token Key – the same for all tokens for a given User; Different for different Users
Authentication
Client generates Authentication Data based on Token Key and PIN
Authentication Data based on Token Key and PIN
Server verifies authentication data and confirms authentication
Encryption
Client generates unique Server-side key component,
Generates unique Encryption key using that component,
Token Key and PIN.
Client Encrypts the data using that encryption Key,
Client transmits to the Server Encrypted Data Entry and Server – Side key component
Server
Decryption
Client retrieves from the Server-side key component and encrypted Data;
Client re-creates the Encryption Key for the Data Entry;
Client decrypts the Data Entry
Encrypted Data Entry
Server – side Key Component (unique for each Data Entry)
Generate
Unique Data Entry Encryption Key

Fig 2.

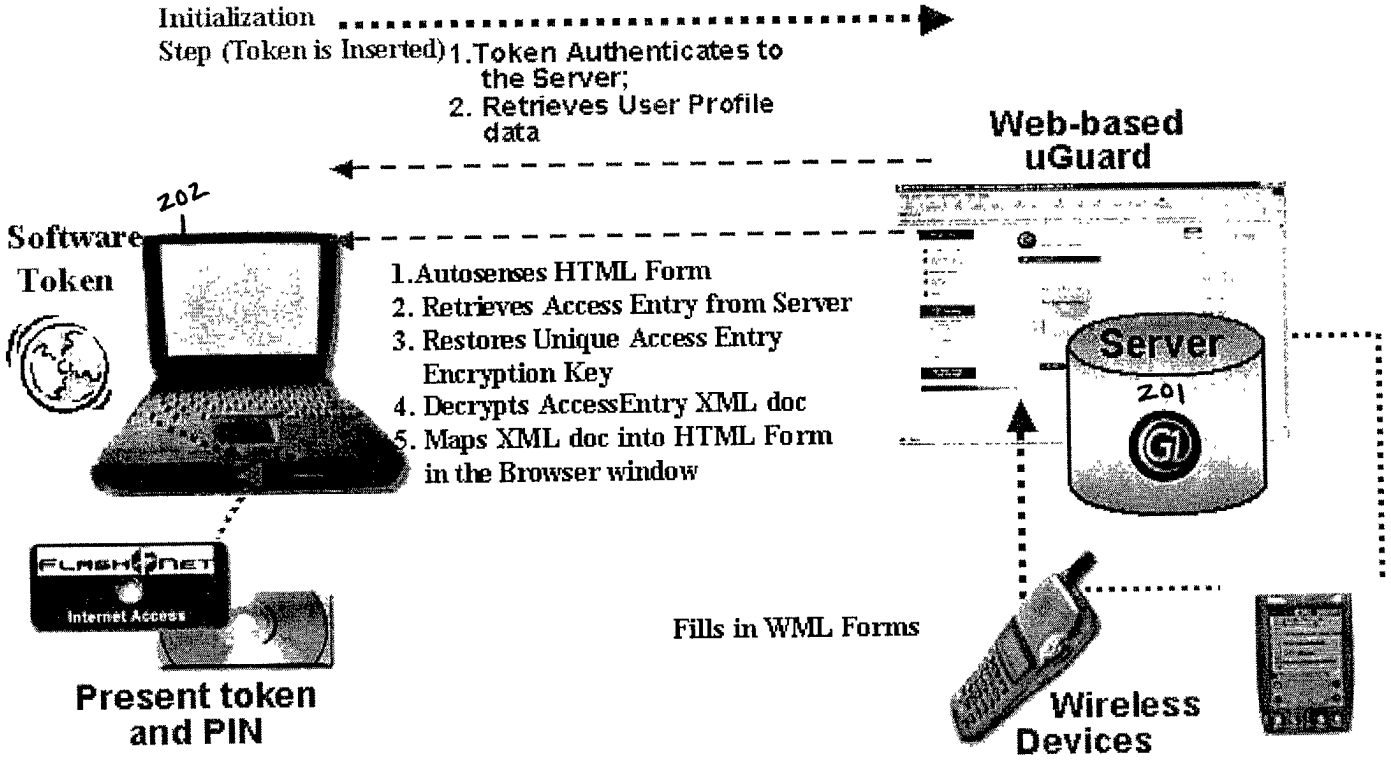

Initialization Step (Token is Inserted)
1. Token Authenticates to the Server;
2. Retrieves User Profile data
Web-based uGuard
202
Software Token
1. Autosenses HTML Form
2. Retrieves Access Entry from Server
3. Restores Unique Access Entry Encryption Key
4. Decrypts AccessEntry XML doc
5. Maps XML doc into HTML Form in the Browser window
Server
201
Internet Access
Present token and PIN
Fills in WML Forms
Wireless Devices

Fig. 3.

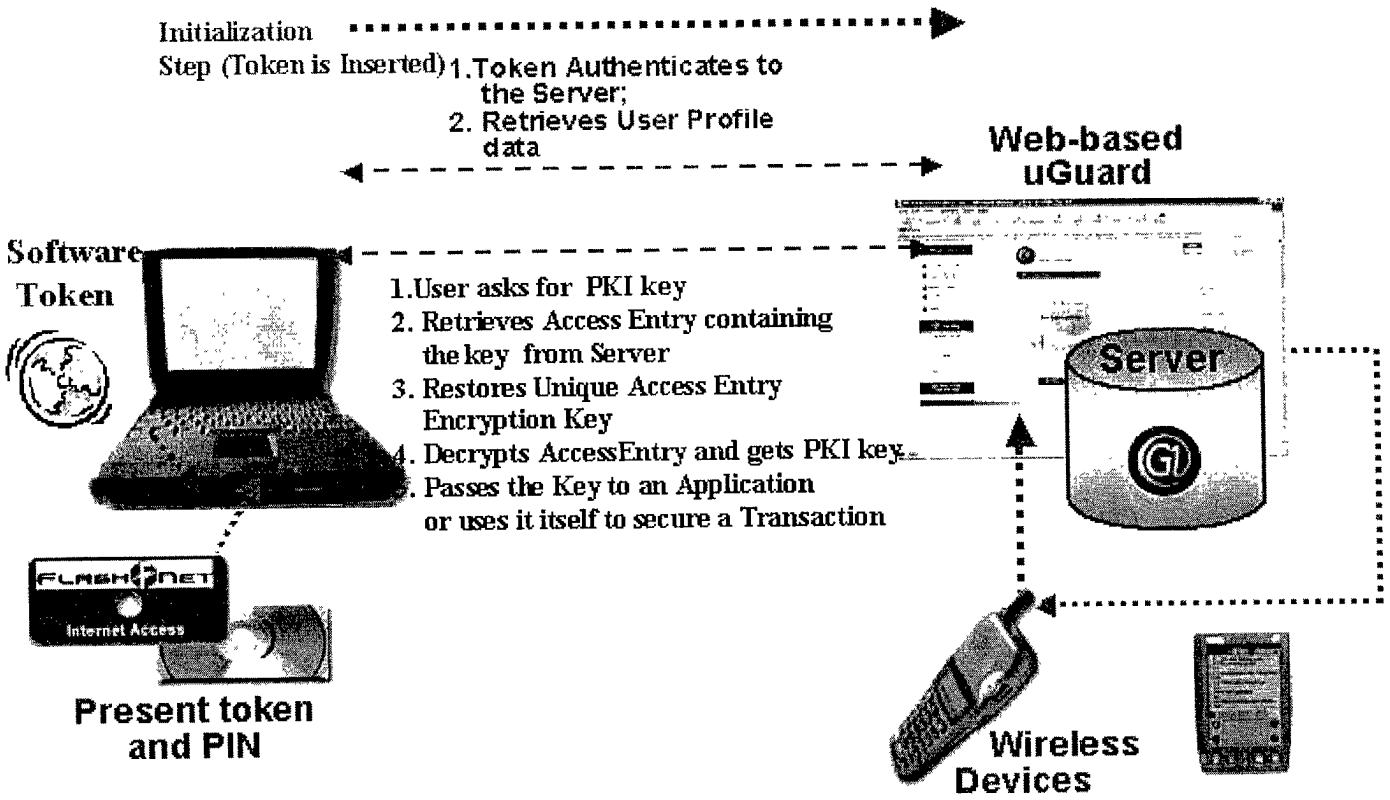
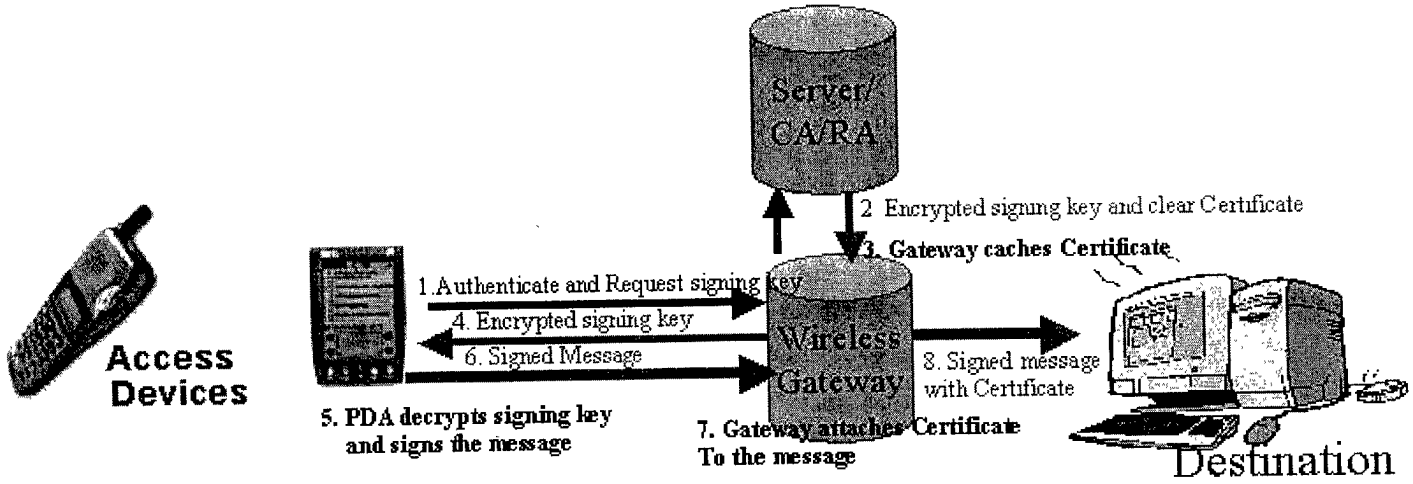

Initialization
Step (Token is Inserted)
1.Token Authenticates to the Server;
2. Retrieves User Profile data
Web-based uGuard
Software Token
1.User asks for PKI key
2. Retrieves Access Entry containing the key from Server
3. Restores Unique Access Entry Encryption Key
4. Decrypts AccessEntry and gets PKI key
5. Passes the Key to an Application or uses it itself to secure a Transaction
Server
Present token and PIN
Wireless Devices

Fig.4.


Server/
CA/RA
2 Encrypted signing key and clear Certificate
3. Gateway caches Certificate
1.Authenticate and Request signing key
4. Encrypted signing key
6. Signed Message
Wireless
Gateway
8. Signed message
with Certificate
Access
Devices
5. PDA decrypts signing key
and signs the message
7. Gateway attaches Certificate
To the message
Destination

500

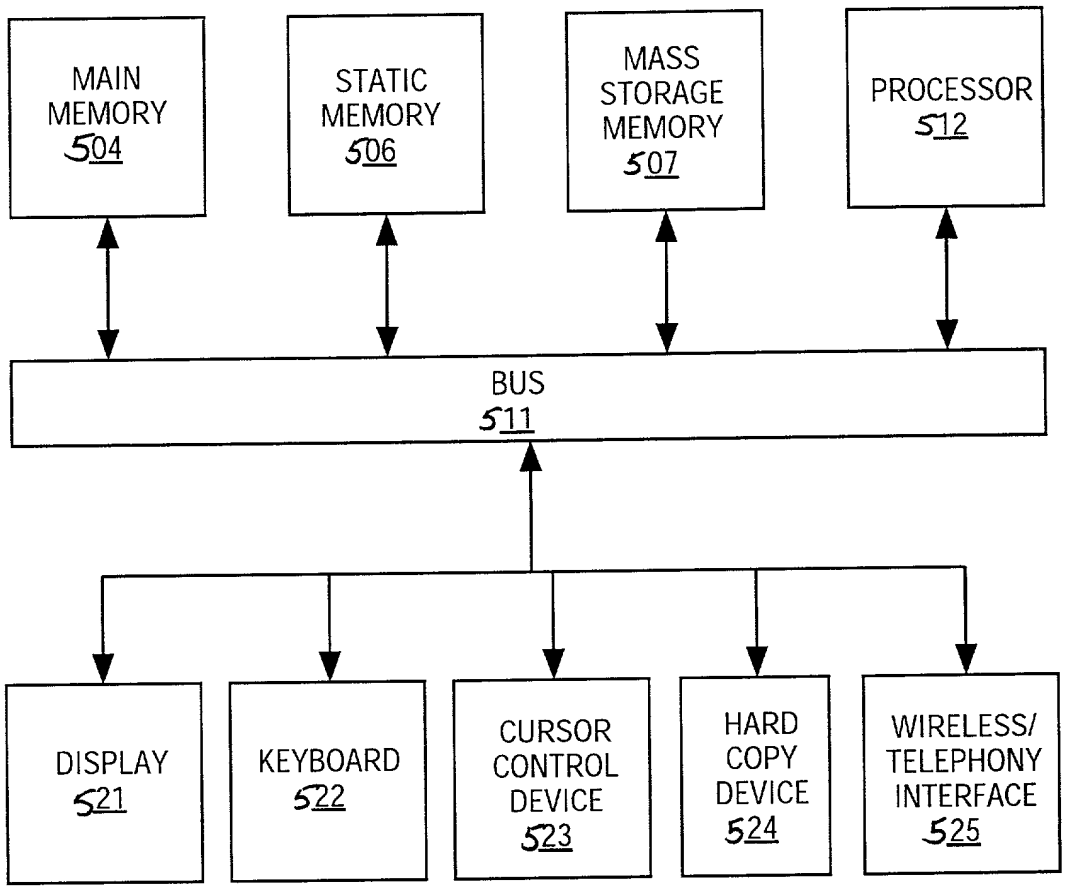

MAIN MEMORY 504
STATIC MEMORY 506
MASS STORAGE MEMORY 507
PROCESSOR 512
BUS 511
DISPLAY 521
KEYBOARD 522
CURSOR CONTROL DEVICE 523
HARD COPY DEVICE 524
WIRELESS/ TELEPHONY INTERFACE 525

FIG. 5